cofc

520.39632VX1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	S. FURUYA, et al
U.S. Patent No.	7,200,232
Serial No.:	09/818,567
Filed:	March 28, 2001
For:	METHOD AND APPARATUS FOR SYMMETRIC-KEY DECRYPTION (Amended)

REQUEST FOR CERTIFICATE OF CORRECTION UNDER 37 CFR §1.323

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

December 3, 2007

Sir:

Pursuant to 35 USC §254, Applicants respectfully request that a Certificate of Correction be issued in connection with the above-referenced application to correct the error noted on the attached Form PTO-1050.

Upon review of the claims, particularly claims 9, 21 and 33 of the application renumbered claims 1, 5 and 10 of the Issued Patent, Applicants noted that the claims were not amended as per the Examiner's Amendment dated March 1, 2007 (copy attached). The present Certificate of Correction incorporates the amendments as per the Examiner's Amendment dated March 1, 2007 so as to improve the language in the claims to fully apprise the public of the meets and bounds of the invention.

The above described errors in claims 1, 5 and 10 of the Issued Patent intended to be modified by the Examiner are minor in character and such errors occurred in good faith without any intent to deceive the Examiner or the

public as to the meets and bounds of the invention on the part of the Applicants. Applicants submit that correction of these errors as set forth above does not involve any changes in the patent that would constitute new matter or require re-examination. The corrections would simply place the claims in the condition intended by the Examiner.

Thus, the present Request for Certificate of Correction complies with the requirements of 35 USC §255 and 37 CFR §1.323. Therefore, entry of the Request for Certificate of Correction is respectfully requested.

Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C., Deposit Account No. 50-1417 (520.39632VX1).

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.

Carl I. Brundidge
Registration No. 29,621

CIB/jdc
(703) 684-1120

PTO/SB/44 (02-01)
Approved for use through 01/31/2004. OMB 0651-0033
United States Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.
(Also Form PTO-1050)

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO: 7,200,232

DATED: April 3, 2007

INVENTOR(s): S. FURUYA, et al

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Please amend claims 9, 21 and 33 as follows:

-- 9. (currently amended)A symmetric-key decryption method performed by a computer, comprising the steps of:

dividing a ciphertext, which is an input text, to generate a plurality of ciphertext blocks each having a predetermined length;

generating a first random number block and a second random number block both corresponding to each of said plurality of ciphertext blocks based on a secret key that is an input value;

performing decryption operations for producing plaintext blocks each corresponding to each of said plurality of ciphertext blocks;

concatenating a series of said ciphertext blocks one after another sequentially to output a plaintext, which includes a message and redundancy data; and

examining the redundancy data to detect whether the plaintext obtained from the ciphertext has been altered,

wherein one of said decryption operations for producing a plaintext block i corresponding to a ciphertext block i (~~2 ≤i, i being~~ 2<=i<= a number indicative of ciphertext blocks) comprises:

a first operation step for performing an arithmetic computation on said ciphertext block i,

a first operation step for performing an arithmetic computation on said ciphertext block i,

a second operation step for performing an arithmetic computation on a result of said first operation step performed on said ciphertext block i and said first random number block corresponding to said ciphertext block i, and

a third operation step for performing an arithmetic computation on a result of said second operation step performed on said ciphertext block i and said second random number block corresponding to said ciphertext block i, to produce said plaintext block i, and

wherein said first operation step performs the arithmetic computation on said ciphertext block i and a result of said second operation step performed on the ciphertext block i-1, and

wherein either said first random number or said second random number is generated in complete isolation from any one of said plurality of ciphertext blocks or the result of said first operation step. --

-- 21. (currently amended)A symmetric-key decryption apparatus comprising:

a circuit for dividing a ciphertext, which is an input text, to generate a plurality of ciphertext blocks each having a predetermined length;

a random number generation circuit for generating a first random number block and a second random number block both corresponding to each of said plurality of ciphertext blocks based on a secret key that is an input value;

a decryption operation circuit for performing decryption operations to produce plaintext blocks each corresponding to each of said plurality of ciphertext blocks;

a circuit for concatenating a series of said plaintext blocks one after another sequentially to output a plaintext, which includes a message and redundancy data; and

a circuit for examining the redundancy data to detect whether the plaintext obtained from ciphertext has been altered,

wherein said decryption operation circuit for producing a plaintext block i corresponding to the ciphertext block i (~~2 ≤i, i being~~ 2<=i<= a number indicative of ciphertext blocks) comprises:

a first circuit for performing a first operation on said ciphertext block i,

a second circuit for performing a second operation on a result of said first operation performed on said ciphertext block i and said first random block corresponding to said ciphertext block i, and

a third circuit for performing a third operation on a result of said second operation performed on said ciphertext block i and said second random number block corresponding to said ciphertext block i, to produce a result of said third operation as said plaintext block i, and

wherein said first circuit performs the first operation on said ciphertext block i and a result of said second operation performed on said ciphertext block i-1, and

wherein either said first random number or said second random number, which is generated by said random number generation circuit, is generated in

complete isolation from any one of said plurality of ciphertext blocks or the result of said first operation. --

-- 33. (currently amended)A medium storing a program for causing a computer to perform a symmetric-key decryption method, wherein said program is read into said computer, said program when executed causes said computer to perform the steps of:

dividing a ciphertext, which is an input text, to generate a plurality of ciphertext blocks each having a predetermined length;

generating a first random number block and a second random number block both corresponding to each of said plurality of ciphertext blocks based on a secret key that is an input value;

performing decryption operations for producing plaintext blocks each corresponding to each of said plurality of ciphertext blocks;

concatenating a series of said plaintext blocks one after another sequentially to output a plaintext, which includes a message and redundancy data; and

examining the redundancy data to detect whether the plaintext obtained from the ciphertext has been altered,

wherein one of said decryption operations for producing a plaintext block i corresponding to a ciphertext block i (~~2 <i, i being~~2<=i<= a number indicative of ciphertext blocks) comprises:

a first operation step for performing an arithmetic computation on said ciphertext block i,

a second operation step for performing an arithmetic computation on a result of said first operation step performed on said ciphertext block i and said first random

number block corresponding to said ciphertext block i; and

a third operation step for performing an arithmetic computation on a result of said second operation step performed on said ciphertext block i and said second random number block corresponding to said ciphertext block i, to produce said plaintext block i, and

wherein said first operation step performs the arithmetic computation on said ciphertext block i and a result of said second operation step performed on the ciphertext block i-1, and

wherein either said first random number or said second random number is generated in complete isolation from any one of said plurality of ciphertext blocks or the result of said first operation step. --

MAILING ADDRESS OF SENDER Carl I. Brundidge, Esq.
MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.
1800 Diagonal Road – Suite 370
Alexandria, VA 22314

PATENT NO: 7,200,232 B2

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

C1B

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/818,567	03/28/2001	Soichi Furuya	520.39632VX1	4795

24956 7590 03/01/2007

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.
1800 DIAGONAL ROAD
SUITE 370
ALEXANDRIA, VA 22314

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
03/01/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

5 2007

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.

EXAMINER

ART UNIT	PAPER

20070223

DATE MAILED:

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

The attached Examiners Amendment to correct typographical errors in the independent claims, please enter entire claim set.

KAMBIZ ZAND
PRIMARY EXAMINER

IN THE CLAIMS

This listing of the claim will replace all prior versions and listings of claim in the present application.

Listing of Claims

Claims 1-8 (canceled).

9. (currently amended)A symmetric-key decryption method performed by a computer, comprising the steps of:

dividing a ciphertext, which is an input text, to generate a plurality of ciphertext blocks each having a predetermined length;

generating a first random number block and a second random number block both corresponding to each of said plurality of ciphertext blocks based on a secret key that is an input value;

performing decryption operations for producing plaintext blocks each corresponding to each of said plurality of ciphertext blocks;

concatenating a series of said ciphertext blocks one after another sequentially to output a plaintext, which includes a message and redundancy data; and

examining the redundancy data to detect whether the plaintext obtained from the ciphertext has been altered,

wherein one of said decryption operations for producing a plaintext block i corresponding to a ciphertext block i (~~2 ≤i, i being~~ 2<=i<= a number indicative of ciphertext blocks) comprises:

a first operation step for performing an arithmetic computation on said ciphertext block i,

a second operation step for performing an arithmetic computation on a

result of said first operation step performed on said ciphertext block i and said first random number block corresponding to said ciphertext block i, and

a third operation step for performing an arithmetic computation on a result of said second operation step performed on said ciphertext block i and said second random number block corresponding to said ciphertext block i, to produce said plaintext block i, and

wherein said first operation step performs the arithmetic computation on said ciphertext block i and a result of said second operation step performed on the ciphertext block i-1, and

wherein either said first random number or said second random number is generated in complete isolation from any one of said plurality of ciphertext blocks or the result of said first operation step.

10. (previously presented) The symmetric-key decryption method as claimed in claim 9, wherein the step of generating random number blocks divides a random number sequence longer than said ciphertext to produce the random number blocks independent of any one of said ciphertext blocks.

11. (original) The symmetric-key decryption method as claimed in claim 10, further comprising steps of:

concatenating a plurality of said plaintext blocks to generate plaintext;

extracting redundancy data included in said plaintext; and

checking said redundancy data to detect whether said ciphertext has

been altered.

12. (previously presented) The symmetric-key decryption method as claimed in claim 11, further comprising steps of:

extracting secret data included in said plaintext, said secret data, different from either said redundancy data or said message, being data generated based on said secret key; and

checking said redundancy data and said secret data to detect whether said ciphertext has been altered.

Claims 13-20 (canceled).

21. (currently amended)A symmetric-key decryption apparatus comprising:

a circuit for dividing a ciphertext, which is an input text, to generate a plurality of ciphertext blocks each having a predetermined length;

a random number generation circuit for generating a first random number block and a second random number block both corresponding to each of said plurality of ciphertext blocks based on a secret key that is an input value;

a decryption operation circuit for performing decryption operations to produce plaintext blocks each corresponding to each of said plurality of ciphertext blocks;

a circuit for concatenating a series of said plaintext blocks one after another sequentially to output a plaintext, which includes a message and

redundancy data; and

a circuit for examining the redundancy data to detect whether the plaintext obtained from ciphertext has been altered,

wherein said decryption operation circuit for producing a plaintext block i corresponding to the ciphertext block i (~~2 <=i, i being~~ 2<=i<= a number indicative of ciphertext blocks) comprises:

a first circuit for performing a first operation on said ciphertext block i,

a second circuit for performing a second operation on a result of said first operation performed on said ciphertext block i and said first random block corresponding to said ciphertext block i, and

a third circuit for performing a third operation on a result of said second operation performed on said ciphertext block i and said second random number block corresponding to said ciphertext block i, to produce a result of said third operation as said plaintext block i, and

wherein said first circuit performs the first operation on said ciphertext block i and a result of said second operation performed on said ciphertext block i-1, and

wherein either said first random number or said second random number, which is generated by said random number generation circuit, is generated in complete isolation from any one of said plurality of ciphertext blocks or the result of said first operation.

22. (previously presented) The symmetric-key decryption apparatus as claimed in claim 21, wherein said random number generation circuit divides a random number sequence longer than said series of

ciphertext blocks to produce the random number blocks independent of any one of said ciphertext blocks.

23. (previously presented) The symmetric-key decryption apparatus as claimed in claim 22, further comprising:

a circuit for concatenating a plurality of said plaintext blocks to generate plaintext;

a circuit for extracting redundancy data included in said plaintext; and

a circuit for checking said redundancy data to detect whether said ciphertext has been altered.

24. (previously presented) The symmetric-key decryption apparatus as claimed in claim 23, further comprising:

a circuit for extracting secret data included in said plaintext, said secret data, different from either said redundancy data or said message, being data generated based on said secret key,

wherein said circuit for detecting whether said ciphertext has been altered checks said secret data and said redundancy data.

Claims 25-32 (canceled).

33. (currently amended)A medium storing a program for causing a computer to perform a symmetric-key decryption method, wherein said program is read into said computer, said program when executed causes said computer to perform the steps of:

dividing a ciphertext, which is an input text, to generate a plurality of ciphertext blocks each having a predetermined length;

generating a first random number block and a second random number block both corresponding to each of said plurality of ciphertext blocks based on a secret key that is an input value;

performing decryption operations for producing plaintext blocks each corresponding to each of said plurality of ciphertext blocks;

concatenating a series of said plaintext blocks one after another sequentially to output a plaintext, which includes a message and redundancy data; and

examining the redundancy data to detect whether the plaintext obtained from the ciphertext has been altered,

wherein one of said decryption operations for producing a plaintext block i corresponding to a ciphertext block i (~~2 ≤i, i being~~2<=i<= a number indicative of ciphertext blocks) comprises:

a first operation step for performing an arithmetic computation on said ciphertext block i,

a second operation step for performing an arithmetic computation on a result of said first operation step performed on said ciphertext block i and said first random number block corresponding to said ciphertext block i; and

a third operation step for performing an arithmetic computation on a result of said second operation step performed on said ciphertext block i and said second random number block corresponding to said ciphertext block i, to produce said plaintext block i, and

wherein said first operation step performs the arithmetic computation

DEC 5 2007

on said ciphertext block i and a result of said second operation step performed on the ciphertext block i-1, and

wherein either said first random number or said second random number is generated in complete isolation from any one of said plurality of ciphertext blocks or the result of said first operation step.

34. (previously presented) The medium storing a program as claimed in claim 33, wherein the step of generating random number blocks divides a random number sequence longer than said ciphertext to produce the random number blocks independent of any one of said ciphertext block.

35. (original) The medium storing a program as claimed in claim 34, wherein said symmetric-key decryption method further comprises steps of:

concatenating a plurality of said plaintext blocks to generate plaintext;

extracting redundancy data included in said plaintext; and

checking said redundancy data to detect whether said ciphertext has been altered.

36. (previously presented) The medium storing a program as claimed in claim 35, wherein said symmetric-key decryption method further comprises steps of:

extracting secret data included in said plaintext, said secret data, different from either said redundancy data or said message, being data generated based on said secret key; and

checking said redundancy data and said secret data to detect whether

said ciphertext has been altered.

Claim 37 (canceled).

38. (previously presented) The symmetric-key decryption apparatus as claimed in claim 22, wherein said random number generation circuit further comprises:

a pseudorandom number generator for generating said random number sequence based on said secret key; and

a circuit for producing said random number blocks from said random number sequence.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/818,567	03/28/2001	Soichi Furuya	520.39632VX1	4795

24956 7590 03/01/2007

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.
1800 DIAGONAL ROAD
SUITE 370
ALEXANDRIA, VA 22314

EXAMINER	
TRAN, ELLEN C	
ART UNIT	**PAPER NUMBER**
2134	

MAIL DATE	DELIVERY MODE
03/01/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

Interview Summary	Application No.	Applicant(s)	
	09/818,567	FURUYA ET AL.	
	Examiner	Art Unit	
	Ellen C. Tran	2134	

All participants (applicant, applicant's representative, PTO personnel):

(1) *Ellen C. Tran*. (3)_____.

(2) *Carl I. Brundidge*. (4)_____.

Date of Interview: *23 February 2007*.

Type: a)☒ Telephonic b)☐ Video Conference
c)☐ Personal [copy given to: 1)☐ applicant 2)☐ applicant's representative]

Exhibit shown or demonstration conducted: d)☐ Yes e)☒ No.
If Yes, brief description: _____.

Claim(s) discussed: *9, 21, and 33*.

Identification of prior art discussed: *N/A*.

Agreement with respect to the claims f)☒ was reached. g)☐ was not reached. h)☐ N/A.

Substance of Interview including description of the general nature of what was agreed to if an agreement was reached, or any other comments: *The purpose of the interview was to enter an amendment to the independent claims to correct typographical errors.*.

(A fuller description, if necessary, and a copy of the amendments which the examiner agreed would render the claims allowable, if available, must be attached. Also, where no copy of the amendments that would render the claims allowable is available, a summary thereof must be attached.)

THE FORMAL WRITTEN REPLY TO THE LAST OFFICE ACTION MUST INCLUDE THE SUBSTANCE OF THE INTERVIEW. (See MPEP Section 713.04). If a reply to the last Office action has already been filed, APPLICANT IS GIVEN A NON-EXTENDABLE PERIOD OF THE LONGER OF ONE MONTH OR THIRTY DAYS FROM THIS INTERVIEW DATE, OR THE MAILING DATE OF THIS INTERVIEW SUMMARY FORM, WHICHEVER IS LATER, TO FILE A STATEMENT OF THE SUBSTANCE OF THE INTERVIEW. See Summary of Record of Interview requirements on reverse side or on attached sheet.

KAMBIZ ZAND
PRIMARY EXAMINER

DEC 5 2007

Examiner Note: You must sign this form unless it is an Attachment to a signed Office action.

Examiner's signature, if required